

IN THE CLAIMS

1. (Currently Amended) A person authentication system for executing person authentication by comparing a template with sampling information, the template being person authentication data, and the sampling information being input by a user, the person authentication system comprising:

a person authentication authority for issuing an electronic person authentication certificate including the template; and

a person authentication execution entity for obtaining ~~the certificate including the~~ template from the electronic person authentication certificate issued by said person authentication authority and executing person authentication on the basis of the obtained template;

wherein the electronic person authentication certificate issued by said person authentication authority stores usage restriction information which includes at least either a certificate expiration date or a certificate usage number limit and includes a template expiration date,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider,

wherein the template is encrypted using a public key of the service provider and extractable from the electronic person authentication certificate using a private key of the service provider, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed,

wherein said person authentication execution entity checks the validity of the electronic person authentication certificate on the basis of the certificate expiration date or the certificate usage number limit when the person authentication is executed on the basis of the electronic person authentication certificate, and

wherein said person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity that received the electronic person authentication certificate, makes a second electronic person authentication certificate in which an

updated certificate expiration date or an updated certificate usage number limit is set according to the request, and then issues the second electronic person authentication certificate.

2. (Previously Presented) A person authentication system according to Claim 1, wherein said person authentication execution entity checks the validity of the electronic person authentication certificate on the basis of the certificate expiration date or the certificate usage number limit in person authentication on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the electronic person authentication certificate has been confirmed on the basis of the certificate expiration date or the certificate usage number limit.

3. (Previously Presented) A person authentication system according to Claim 1, wherein said person authentication execution entity has a person authentication executing device, and the person authentication executing device executes the following processing when usage restriction information of the certificate usage number limit is stored in the electronic person authentication certificate:

storing a set usage count in a memory of the person authentication executing device;

updating usage count data stored in the memory every time the electronic person authentication certificate is used;

determining whether the usage count data is within the limits of the set usage count of the electronic person authentication certificate; and

executing person authentication by comparing user input sampling information with the template stored in the electronic person authentication certificate if the usage count data is within the certificate usage number limit.

4. (Currently Amended) A person authentication system according to Claim 1, wherein the electronic person authentication certificate issued by said person authentication authority stores the a template expiration date which is information on an expiration date of the template stored in the electronic person authentication certificate; and

said person authentication execution entity checks the validity of the template on the basis of the template expiration date in person authentication on the basis of the electronic person authentication certificate.

5. (Canceled).

6. (Currently Amended) A person authentication system according to Claim 1, wherein said person authentication execution entity functions as an information processing apparatus, and the information processing apparatus checks the validity of the a template expiration date or the certificate expiration date of an electronic person authentication certificate which is set in the certificate stored in the information processing apparatus and then outputs a request for issuing the electronic person authentication certificate to said person authentication authority which issues the electronic person authentication certificate when the validity can not be confirmed;

said person authentication authority makes the electronic person authentication certificate in which an expiration date is set and then issues the electronic person authentication certificate to the information processing apparatus; and

the information processing apparatus has storage means and stores the electronic person authentication certificate, which is issued by said person identification certificate authority, in the storage means.

7. (Currently Amended) A person authentication system according to Claim 1, wherein said person authentication authority checks the validity of the a template expiration date or an expiration date of an issued electronic person authentication certificate, and then gives notice to an entity receiving the electronic person authentication certificate that the template expiration date or the certificate expiration date is approaching.

8. (Canceled).

9. (Previously Presented) A person authentication system according to Claim 1, wherein said person authentication authority receives a request for updating the template, stored in the electronic person authentication certificate which has been issued, from an authenticated user of the electronic person authentication certificate; and

wherein said person authentication authority nullifies the electronic person authentication certificate according to the request and then makes the second electronic person authentication certificate on the basis of an updated template.

10. (Currently Amended) A person authentication system according to Claim 1, wherein said person authentication authority receives data of a request for setting the a template expiration date from an authenticated user of the electronic person authentication certificate, and then makes the second electronic person authentication certificate in which the template expiration date is set on the basis of the data of the request for setting the template expiration date.

11. (Previously presented) A person authentication system according to Claim 1, wherein said person authentication authority and said person authentication executing entity execute mutual authentication, when data communication is performed therebetween, a data transmitter puts a digital signature on transmitted data, and a data receiver verifies the digital signature.

12. (Previously presented) A person authentication system according to Claim 1, wherein the template is at least one of personal biotic information, personal nonbiotic information, and a password,

wherein the personal biotic information is selected from at least one of the group consisting of fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information, and

wherein the personal nonbiotic information is selected from at least one of the group consisting of seal information, passport information, driver's license information, and card information.

13. (Previously Presented) A person authentication system according to Claim 1, wherein said person authentication authority puts a digital signature on the electronic person authentication certificate issued by said person authentication authority.

14. (Currently Amended) A person authentication method for executing person authentication by comparing a template with sampling information, the template being person authentication data, and the sampling information being input by a user, the person authentication method comprising:

causing a person authentication authority to issue an electronic person authentication certificate including the template;

causing a person authentication execution entity to obtain ~~the certificate including~~ the template from the electronic person authentication certificate issued by the person authentication authority and to execute person authentication on the basis of the obtained template;

storing usage restriction information, which includes at least either a certificate expiration date or a certificate usage number limit, in the electronic person authentication certificate issued by the person authentication authority, the electronic person authentication certificate including a template expiration date; and

causing the person authentication execution entity to check the validity of the electronic person authentication certificate on the basis of the certificate expiration date or the certificate usage number limit in person authentication on the basis of the electronic person authentication certificate,

wherein the person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity receiving the electronic person authentication certificate, then makes a second electronic person authentication certificate in which an expiration date or an updated certificate usage number limit is set according to the request, and issues the second electronic person authentication certificate,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider, and

wherein the template is encrypted using a public key and extractable from the electronic person authentication certificate using a private key, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed.

15. (Previously Presented) A person authentication method according to Claim 14, wherein the person authentication execution entity checks the validity of the electronic person authentication certificate on the basis of the certificate expiration date or the certificate usage number limit in person authentication on the basis of the electronic person authentication

certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the electronic person authentication certificate has been confirmed on the basis of the certificate expiration date or the certificate usage number limit.

16. (Previously Presented) A person authentication method according to Claim 14, wherein the person authentication execution entity has a person authentication executing device, and the person authentication executing device executes the following processing when usage restriction information of the certificate usage number limit is stored in the electronic person authentication certificate:

storing a set usage count in a memory of the person authentication executing device;

updating usage count data stored in the memory every time the electronic person authentication certificate is used;

determining whether the usage count data is within the limits of the set usage count of the electronic person authentication certificate; and

executing person authentication by comparing sampling information, input by a user, with the template stored in the electronic person authentication certificate if the usage count data is within the limits.

17. (Currently Amended) A person authentication method according to Claim 14, wherein the person authentication authority stores the a template expiration date, which is information on an expiration date of the template stored in the electronic person identification certificate made by the person authentication authority; and

a person authentication execution entity checks the validity of the template on the basis of the template expiration date in person authentication on the basis of the electronic person authentication certificate.

18. (Canceled).

19. (Currently Amended) A person authentication method according to Claim 14, wherein said person authentication execution entity functions as an information processing apparatus;

the information processing apparatus checks the validity of the a template expiration date or a certificate expiration date of the electronic person authentication certificate which is set in the electronic person authentication certificate stored in the information processing apparatus, and then outputs a request for issuing the electronic person authentication certificate to the person authentication authority which issues the electronic person authentication certificate when the validity can not be confirmed;

the person authentication authority makes the electronic person authentication certificate in which a new certificate expiration date is set and then issues the electronic person authentication certificate to the information processing apparatus; and

the information processing apparatus has storage means and stores the electronic person authentication certificate, which is issued by the person authentication authority, in the storage means.

20. (Currently Amended) A person authentication method according to Claim 14, wherein the person authentication authority checks the validity of the a template expiration date or an expiration date of the issued electronic person authentication certificate, and then gives notice to an entity receiving the electronic person authentication certificate that the template expiration date or the certificate expiration date is approaching.

21. (Canceled).

22. (Previously Presented) A person authentication method according to Claim 14, wherein the person authentication authority receives a request for updating the template, stored in the electronic person identification certificate which issued, from an authenticated user of the electronic person authentication certificate; and

wherein the person authentication authority nullifies the electronic person authentication certificate according to the request and then makes the second electronic person authentication certificate on the basis of the updated template.

23. (Currently Amended) A person authentication method according to Claim 14, wherein the person authentication authority receives data of a request for setting the a template expiration date from an authenticated user of the electronic person authentication certificate, and then makes the second electronic person authentication certificate in which the template

expiration date is set on the basis of the data of the request for setting the template expiration date.

24. (Previously presented) A person authentication method according to Claim 14, wherein the person authentication authority and the person authentication executing entity execute mutual authentication, when data communication is performed therebetween, a data transmitter puts a digital signature on transmitted data, and a data receiver verifies the digital signature.

25. (Currently Amended) An information processing apparatus for executing person authentication by comparing a template with sampling information, the template being person authentication data, and the sampling information being input by a user, the information processing apparatus comprising:

a section for storing the template in an electronic person authentication certificate to execute person authentication on the basis of the electronic person authentication certificate issued by a person authentication certificate authority which is a third party, the electronic person authentication certificate storing at least one of a certificate expiration date and a certificate usage number limit and stores a template expiration date; and

a section for checking the validity of the electronic person authentication certificate on the basis of the certificate expiration date or the certificate usage number limit in person authentication on the basis of the electronic person authentication certificate, and then executing the person authentication by comparing the template, stored in the electronic person authentication certificate, with the sampling information input by the user on the condition that the validity of the electronic person authentication certificate has been confirmed on the basis of the certificate expiration date or the certificate usage number limit,

wherein the person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity that received the electronic person authentication certificate, makes a second electronic person authentication certificate in which an updated certificate expiration date or an updated certificate usage number limit is set according to the request, and then issues the second electronic person authentication certificate,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using

a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider, and

wherein the template is encrypted using a public key and extractable from the electronic person authentication certificate using a private key, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed.

26. (Currently Amended) An information processing apparatus for executing person authentication by comparing a template with sampling information, the template being person authentication data, and the sampling information being input by a user, the information processing apparatus comprising:

a section for storing the template in an electronic person authentication certificate to execute person authentication on the basis of the electronic person authentication certificate issued by a person authentication certificate authority which is a third party, the electronic person authentication certificate storing at least one of a certificate expiration date and a certificate usage number limit and storing a template expiration date;

a section for executing the following processing when usage restriction information of a valid certificate usage number limit is stored in the electronic person authentication certificate:

storing a set usage count in a memory of the information processing apparatus;

updating the usage count stored in the memory every time the electronic person authentication certificate is used; determining whether the usage count is within the limits of the certificate usage number limit of the electronic person authentication certificate; and

executing person authentication by comparing user input sampling information with the template stored in the electronic person authentication certificate if the usage count in memory is within the limits of the certificate usage number limit,

wherein the person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity that received the electronic person authentication certificate, makes a second electronic person authentication certificate in which an

updated certificate expiration date or an updated certificate usage number limit is set according to the request, and then issues the second electronic person authentication certificate,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider, and

wherein the template is encrypted using a public key and extractable from the electronic person authentication certificate using a private key, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed.

27. (Currently Amended) An information processing apparatus for executing person authentication by comparing a template with sampling information, the template being person authentication data, and the sampling information being input by a user, the information processing apparatus comprising:

a section for storing the template in an electronic person authentication certificate to execute person authentication on the basis of the electronic person authentication certificate issued by a person authentication certificate authority which is a third party, the electronic person authentication certificate storing at least one of a certificate expiration date and a certificate usage number limit and stores a template expiration date; and

a section for checking the validity of the template on the basis of a template expiration date in person authentication on the basis of the electronic person authentication certificate, and then executing the person authentication by comparing the template, which is stored in the electronic person authentication certificate, with the sampling information input by the user on a condition that validity of the template expiration date has been confirmed,

wherein the person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity that received the electronic person authentication certificate, makes a second electronic person authentication certificate in which an

updated certificate expiration date or an updated certificate usage number limit is set according to the request, and then issues the second electronic person authentication certificate,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider, and

wherein the template is encrypted using a public key and extractable from the electronic person authentication certificate using a private key, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed.

28. (Currently Amended) A program providing medium for proving a computer program which executes person authentication on the computer program by comparing a template stored in an electronic person authentication certificate with sampling information, the template being person authentication data, and the sampling information being input by a user, the computer program comprising:

a step of confirming whether usage restriction information, which includes either a certificate expiration date, a certificate usage number limit, or a template expiration date, is stored in the electronic person authentication certificate issued by a person authentication authority;

a step of checking the validity of the electronic person authentication certificate on the basis of the certificate expiration date, the certificate usage number limit, or the template expiration date in person authentication on the basis of the electronic person authentication certificate; and

a step of executing the person authentication by comparing the template, which is stored in the electronic person authentication certificate, with the sampling information input by the user on a condition that the validity of the electronic person authentication certificate has been confirmed on the basis of the certificate expiration date, certificate usage number limit, or the template expiration date,

wherein the person authentication authority receives a request for updating the issued electronic person authentication certificate from an entity that received the electronic person authentication certificate, makes a second electronic person authentication certificate in which an updated certificate expiration date or an updated certificate usage number limit is set according to the request, and then issues the second electronic person authentication certificate,

wherein when a service provider has a transaction with a user, the person authentication authority issues the electronic person authentication certificate including a signature written using a private key of the person authentication authority, and the signature is verifiable using a public key of the person authentication authority that is stored by the service provider, and

wherein the template is encrypted using a public key and extractable from the electronic person authentication certificate using a private key, and after the template is successfully extracted, the person authentication execution entity checks the validity of the template on the basis of the template expiration date when the person authentication is executed on the basis of the electronic person authentication certificate, and then executes the person authentication by comparing the template, stored in the electronic person authentication certificate, with sampling information input by the user on the condition that the validity of the template expiration date has been confirmed.